Making Business-Based Security Investment Decisions – A Dashboard Approach

Julia H. Allen, Software Engineering Institute [vita[1]]

2008-06-25; Updated 2008-09-23

This article presents one approach for selecting security investments using business-based criteria. The approach and supporting tool define seven decision criteria categories, each supported by three or more indicators. Categories and indicators are ranked and applied to a series of investments. Individual investment scores are presented for discussion and evaluation by decision makers. Our intent is that this approach can be use to rationalize and prioritize any class of security investments including software assurance.

Introduction

In today's business climate, we are constantly dealing with the demand to do more with less. The resources required to run the business, let alone to invest in new initiatives, are always at a premium—time, money, staff expertise, information, and facilities, not to mention energy and attention span. All investment decisions are about doing what is best for the organization (and its stakeholders). However, what is best is sometimes hard to define, hard to quantify, and even harder to defend when the demand for investment dollars exceeds the supply.

Business leaders are becoming more aware of the need to invest in information and software assurance—to meet compliance requirements and optimize their total cost of ownership for software-intensive applications and systems. So how do we ensure that security investments are subject to the same decision criteria as other business investments? And by so doing, how are we able to justify investments that increase our confidence in our ability to protect digital information using software that is more able to resist, tolerate, and recover from attack?

One approach may begin to shed some light on this topic. It is based on recent CERT research on how to make well-informed security investment decisions using business-based criteria. Over the past four years, CERT has developed a body of knowledge in enterprise and information security governance, including a detailed framework and implementation guide that describe a robust security governance program[10]. When faced with this framework of tasks, actions, roles and responsibilities, and outcomes, senior leaders say “This is all well and good, but I have many more pressing issues to deal with than security governance. Can you

1. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/215-BSI.html (Allen, Julia H.)
2. #dsy985-BSI_found
3. #dsy985-BSI_dashboard
4. #dsy985-BSI_review
5. #dsy985-BSI_next
6. #dsy985-BSI_appx
7. #dsy985-BSI_a.1
8. #dsy985-BSI_a.2
9. #dsy985-BSI_a.3
10. http://www.cert.org/governance

provide me with an aid to select and prioritize these and other security-related actions that I can use as an input to normal planning and capital investment processes?"

This article describes one such approach that is in early demonstration and pilot testing. Organizations that have participated in reviews and initial pilot projects represent the commercial, defense contracting, U.S. federal agency, non-profit, and security vendor sectors. Our intent in presenting it here is to obtain additional feedback about whether it serves as a promising structure and tool for making business-based investment decisions in information and software assurance.

Foundation and Structure

The Security Investment Decision Dashboard (SIDD) provides a means for evaluating and comparing several candidate security investments.[11] A foundational principle of the dashboard is that the priorities for candidate investments are driven by the organization's *desired outcome for any given investment*, not just security investments. This ensures that security investments are subject to the same decision criteria as other business investments. They can then be presented, reviewed, analyzed, debated, and compared using the same scales, factors, and investment-selection criteria and processes.

SIDD describes seven decision criteria *categories*, each supported by three or more decision *indicators*, totaling 33 in all. Two CERT reports [Allen 05[12], Westby 07[13]] served as the starting point for selecting business-based criteria that could be used to evaluate candidate investments. A number of relevant business and security sources [Campbell 06[14], CISWG 05[15], Drugescu 06[16], ISO 07[17], Kleinfeld 06[18]] were analyzed for business-based questions and factors that could help inform security investment decisions. The collected set of questions and factors are reflected in the current set of 33 indicators. The seven categories were derived through affinity grouping of the 33 indicators.

Each category is described in the form of one or two questions to ask. Categories are presented in shaded text in Table 1[19] and include Cost, Criticality & Risk, Feasibility, Positive Interdependencies, Involvement, Measurability, and Time & Effort Required. The importance of each category is determined by considering the question "What should *any* candidate investment do for the organization and its stakeholders?" or alternatively, "What is the basis or criteria for selecting *any* candidate investment?"

For example, is it most important that an investment (1) be low cost, (2) be critical to meet business objectives or mitigate a high degree of risk, or (3) be feasible in terms of likelihood of success? The questions in Table 1 define each category. Priorities or rankings are then assigned to the category based on the importance of the category to the organization's investment selection process. Each category is further elaborated by three or more indicators that are listed following each category in Table 1. This is a "starter set" that can be tailored to reflect a specific organization's decision factors.

Table 1. SIDD categories and indicators

11. Some reviewers have suggested that SIDD could be useful for other types of business investments. See the "Initial Review Comments and Potential Uses" section below.
12. http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/management/564-BSI.html#dsy564-BSI_wp1012117 (Governance and Management References)
13. http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/management/564-BSI.html#dsy564-BSI_Westby07 (Governance and Management References)
14. http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/management/564-BSI.html#dsy564-BSI_camp06 (Governance and Management References)
15. http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/management/564-BSI.html#dsy564-BSI_CISWG05 (Governance and Management References)
16. http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/management/564-BSI.html#dsy564-BSI_Drugescu06 (Governance and Management References)
17. http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/management/564-BSI.html#dsy564-BSI_ISO/IEC07 (Governance and Management References)
18. http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/management/564-BSI.html#dsy564-BSI_Kleinfeld06 (Governance and Management References)
19. #dsy985-BSI_table1

Category	Indicator
Cost	What is the estimated total cost to accomplish this investment, taking into account the potential cost savings and/or risk reduction to the organization?
	Overt cost in dollars at outset to accomplish this investment?
	Estimated life cycle cost in dollars over time to sustain this investment?
	Cost of NOT doing this investment, in terms of potential exposure and residual risk (high = investment is more necessary)?
	Potential cost savings to organization beyond breakeven point, if quantifiable (ROI), over time (high = better)?
Criticality & Risk	What is the degree to which this investment contributes to meeting the organization's business objectives and risk management goals?
	Degree to which this investment is key or mainstream in helping the organization meet its primary objectives and critical success factors?
	Degree of risk (as assessed in terms of likelihood and potential impact—high/medium/low priority) mitigated by this investment?
	Degree to which this investment helps the organization protect stakeholders' (shareholders') interests?

Feasibility	How likely is this investment to succeed?
	Likelihood of success on first try?
	Likelihood of success on subsequent tries (if first try fails)?
	Likelihood that turnover among management and/or board of directors will negate work expended on this investment (low likelihood = better)?
	Likelihood that this investment will need to be rolled back (low = better)?

Positive Interdependencies	(1) To what degree does this investment integrate with or represent reasonable changes to existing organizational processes and practices, rather than requiring new ones? (2) To what degree does this investment pave the way for future investments (compliance, policy, risk management, etc.)?
	Degree to which other investments/tasks are dependent on this one (i.e., degree to which this investment makes it easier to accomplish additional tasks)?
	Degree to which the accomplishment of this investment makes it easier to comply with **current** laws and regulations?
	Degree to which the accomplishment of this investment makes it easier to comply with potential **new** laws and regulations in the future?
	Degree to which existing knowledge and/or skills can be used to accomplish this investment, rather than requiring new skills/knowledge?
	Degree to which this investment produces positive side effects (e.g., enhancing brand/reputation, building customer trust, benefiting supply chain partners)?

Involvement	What level of involvement and buy-in are required from various parties for investment success—both within and outside of the organization?
	Level of buy-in required throughout the organization? (Must all employees be on board 100% for this to work? Or only a subset, such as management and certain key employees?)
	To what extent does this investment require the active involvement of many departments across the organization?
	Number of people who need to be actively involved?
	Level of involvement by third parties required (partners, consultants, vendors, etc.)?
	Degree of external, independent assessment/auditing (vs. in-house assessment/auditing) required?

Measurability	How measurable is the outcome of this investment?
	Degree to which this investment can be evaluated using existing approaches and reporting mechanisms?
	What is the measurability of the outcome? Can it be quantified in tangible terms (revenue, market share, stock price, etc.)?
	If the outcome is intangible (e.g., goodwill, increased customer trust, enhanced brand), can the benefits be demonstrated against meaningful business success factors?

Time & Effort Required	(1) What level of staff-hours will be required to accomplish this investment? (2) How long will it take to reach break-even cost for this investment?
	Board of directors time required?
	Senior management time required?
	Cross-organizational team/steering committee time required?
	Middle and lower management time required?
	Other key staff time required?
	Time likely needed to achieve the required level of buy-in?
	Time required to achieve first demonstrated results?
	Time required to achieve full adoption and use of the investment results across all affected business units?
	Time to achieve breakeven, if quantifiable?

A business leader may determine that there are other factors or different factors that they use in their investment decision making processes. The SIDD is designed so that categories and indicators can be changed, added, and deleted, and the dashboard will continue to present meaningful comparisons.

Dashboard results are presented in a comparative bar graph form (see Appendix A.3[20] for an example). Score totals are presented for the 7 categories and the 33 indicators for each investment. An additional result is calculated for the 6 indicators ranked highest (1-6). This result has been included to accommodate the situation where a subset of indicators is important for investment selection as a companion to the total scores for all categories and for all indicators.

20. #dsy985-BSI_a.3

Using the Dashboard

Investment priorities and comparative scores are determined using a two-phased approach. In Phase 1, a decision maker prioritizes categories (Step 1) and indicators (Step 2). The idea here is to determine the importance of each category and each indicator when making *any* organizational investment decision. These priorities (or rankings) will be applied to all candidate investments during Phase 2.

Phase 2 defines the candidate investments that are to be evaluated (Step 3). There is no upper bound but typically 3-5 investments are evaluated in one use of the dashboard. The decision maker then answers the category and indicator questions (Step 4) for each investment. Scores are calculated by applying the priorities specified in Phase 1 to these answers. Each step is further described below. An example dashboard entry for each step is presented in Appendix A[21].

1. Phase 1: Establish priorities for all types of organizational investments

   Step 1: Rank categories 1-7 (shaded entries in Table 1[22]) based on their relative importance for any organizational investment decision, 1 being most important and 7 being least important. Do not consider any specific security investment when performing this ranking. An example category ranking appears in Appendix A.1[23].

   Step 2: Rank indicators 1-33 (more detailed entries in Table 1[24]), again, based on their relative importance for any organizational investment decision with a ranking of "1" as the most important. Given that 33 indicators is a long list to prioritize, some reviewers grouped these into three sets of ten and then ranked the group of ten. Others created larger scale granularity by assigning a value of, say, 1, 5, or 10 to all 33, which then produced a larger numeric difference between investment scores. An example indicator ranking appears in Appendix A.1[25].

   The current version of the dashboard does not enforce a correlation between category and indicator rankings. This means that one category could be ranked as having the highest priority, while indicators in other categories could be ranked as being more important.

   Steps 1 and 2 are intended to be done once and then applied during all subsequent investment analyses. This helps ensure that results are based on the same ranking and thus can be meaningfully compared. Rankings are periodically reviewed during normal planning cycles or following key events (such as a merger or acquisition) to ensure that they continue to reflect current business priorities.

   Some reviewers have suggested that one or more senior C-level leaders perform the category ranking

21. #dsy985-BSI_appx

and another group, such as a cross-organizational steering committee, performs the indicator rankings. When category and indicator rankings are done independently, these can then be compared to see if they are consistent or reveal misunderstandings or differences of opinion. In several cases, the shared understanding that resulted from doing these rankings was of equal or greater value than the dashboard results.

2. Phase 2: Evaluate each investment

For each candidate security investment:

Step 3: Define the investment so that those evaluating it have a common understanding of its scope and intent. While SIDD has been used to evaluate security governance and IT investments (such as policy development, specifying segregation of duties, developing an asset inventory, deploying wireless, creating a new operations center), four example software assurance investments are selected here and further illustrated in Appendix A[26].

- A – Integrate architectural risk analysis into the standard SDLC.
- B – Integrate secure coding practices for C and C++ into the standard SDLC.
- C – Integrate the use of static code analysis tools into the standard SDLC.
- D – Integrate security requirements engineering using SQUARE[27] into the SDLC.

Deciding to use SIDD assumes that resources are insufficient to start up all of these now, so we use this approach to help inform which ones to fund.

Step 4: Answer the category and indicator questions (Table 1[28]) for each investment by using a dashboard worksheet, one per investment. Determining an answer for each question is accomplished by selecting a value from 1 to 5. Based on the question, answers range from very high to very low or very low to very high. An example of answers for one investment and one category is shown in Appendix A.2[29].

Step 5: Review and discuss the results. An example of summary results for the four example investments appears in Appendix A.3[30].

Dashboard outcomes identify the highest priority (highest scoring) investments based on the category rank, the indicator rank, and the answers to the questions for each investment. Given that the category and

indicator ranks are fixed (and weighted to normalize the scores[31]), the dashboard results can be meaningfully compared and used to help select which investments to fund, as well as providing a defensible rationale for those that were not selected.

If, based on other factors, these highest scoring investment choices are not justified, this is a valuable opportunity to re-examine the category and indicators rankings and answers to determine if they do indeed reflect how the organization makes investment decisions.

This tool is not intended as a substitute for human judgment. It can be used to make judgments more explicit, to apply a consistent set of decision criteria to all investments which can then be communicated, and to capture trends over time.

Initial Review Comments and Potential Uses

This section summarizes some of the feedback based on review and early pilot use of the demonstration version of SIDD. The review process started in September 2007 and is ongoing as of the publication date of this article. These comments come from eight organizations representing large commercial, large defense contracting, not-for-profit, U.S. federal civilian agency, and security consulting/products and services sectors.

Review comments included the following:

- SIDD does a good job in tying information security to business drivers. The phrase that seems to sum this up is "alignment with the business." In my experience this tends to be a real problem, either from the perspective of the Information Security (IS) group actually managing to (or even understanding the importance of) aligning with the business, or from the perspective of the business having a means of determining whether IS does align with their goals. This method provides a simple framework for that to occur.
- SIDD can be used to lend discipline and rigor to a fairly intuitive decision process.
- SIDD is perfect to support presenting a business case, as it creates and documents a defensible argument to senior management. It also aids in thinking through the implications of our decisions.
- If management defines the categories and their ranking in terms of an organization's drivers, a framework is automatically created within which the departments can ensure that their assessments are made in terms of those drivers.
- SIDD is a brilliant tool for helping people use these types of factors (categories and indicators) to justify their control selection process versus, for example, selecting controls to meet an auditor's checklist. It's very difficult to argue against a checklist when you have no alternative.
- The dialogue SIDD stimulates may be of greater value than the actual output.

Reviewers also identified the following potential uses in addition to SIDD’s intended use of comparing among a set of security investments. SIDD could be used to

- Help prioritize risk assessment or security assessment results
- Help identify and prioritize objectives as part of normal annual and strategic planning processes
- Perform IT project portfolio management
- Evaluate a range of vendor proposals and select one
- Measure decision-making trends and capture benchmark data, as well as benchmark and validate investment choices
- Reflect the changing priorities of the business as time goes on
- Perform "what if" and best case/worst case analysis of alternatives
- Encourage fact-based decision making

31. Category and indicator ranks are converted into weights that are used as multipliers to normalize dashboard scores. This is necessary due to a priority of "1" being highest, yet the highest total score reflects the highest priority investment.

- Explicitly capture how leaders make decisions and, as a result, help educate new business leaders and project managers on how the organization selects what investments to resource

Next Steps

Plans for SGDD during CY2008 include continued external review, pilot use, and refinement based on feedback that includes

- expanding the current set of categories and indicators, along with allowing a decision maker to select a reduced set that is most relevant
- exploring approaches for more meaningful visual representations of the SIDD results, examining scorecard and dashboard approaches currently in use
- supporting dynamic, "what-if" decision making based on changing category and indicator priorities
- developing a more robust version of the tool as a standalone application, which will eventually replace the current Excel spreadsheet demonstration version

Once a sufficient number of pilot cases have occurred, we plan to capture and document selected case studies.

Please contact the author for further information or if you wish to participate in this pilot effort.

Appendix A

This appendix contains the following three sections:

- A.1 Category and Indicator Rankings[32]
- A.2 Scores for One Investment in One Category[33]
- A.3 Summary Results for Four Investments[34]

A.1 Category and Indicator Rankings

In this example, the “Criticality and Risk” category is ranked as “1” and is the most important category for any organizational investment decision. “Measurability” is ranked as “7” and is thus the least important category-level criteria.

The indicator that has the highest priority here is the “Cost of NOT doing this investment, in terms of potential exposure and residual risk.” It is ranked as “1” and is the most important indicator for any organizational investment decision. As you might expect, the three indicators under “Measurability” are the least important indicators.

	Category / Indicator	Cat Rank (1-7)	Ind Rank (1-33)
Cat	**Cost**	2	
Consider	What is the estimated total cost in dollars of accomplishing this investment, taking into account the potential cost savings and/or risk reduction to the organization?		
Indicators	Overt cost in dollars at outset to accomplish this investment?		6
	Estimated life cycle cost in dollars over time to sustain this investment?		7
	Cost of NOT doing this investment, in terms of potential exposure and residual risk (high = investment is more necessary)?		1
	Potential cost savings to organization beyond breakeven point, if quantifiable (ROI), over time? (high = better)		9

	Category / Indicator	Cat Rank (1-7)	Ind Rank (1-33)
Cat	**Criticality and Risk**	1	
Consider	What is the degree to which this investment contributes to meeting the organization's business objectives and risk management goals?		
Indicators	Degree to which this investment is key or mainstream in helping the organization meet its primary objectives and critical success factors?		4
	Degree of risk (as assessed in terms of likelihood and potential impact – high/medium/low priority) mitigated by this investment?		3
	Degree to which this investment helps the organization protect stakeholders' (shareholders) interests?		5

	Category / Indicator	Cat Rank (1-7)	Ind Rank (1-33)
Cat	**Feasibility**	3	
Consider	How likely is this investment to succeed?		
Indicators	Likelihood of success on first try?		10
	Likelihood of success on subsequent tries (if first try fails)?		11
	Likelihood that turnover among management and/or board of directors will negate work expended on this investment (low likelihood = better)?		20
	Likelihood that this investment will need to be rolled back (low = better)?		16

	Category / Indicator	Cat Rank (1-7)	Ind Rank (1-33)
Cat	**Positive Interdependencies**	6	
Consider	(1) To what degree does this investment integrate with or represent reasonable changes to existing organizational processes and practices, rather than requiring new ones?		
	(2) To what degree does this investment pave the way for future investments (compliance, policy, risk management, etc.)?		
Indicators	Degree to which other investments/tasks are dependent on this one (i.e., degree to which this investment makes it easier to accomplish additional tasks)?		28
	Degree to which the accomplishment of this investment makes it easier for the organization to comply with **current** laws and regulations?		2
	Degree to which the accomplishment of this investment makes it easier for the organization to comply with potential **new** laws and regulations in the future?		29
	Degree to which existing knowledge and/or skills can be used to accomplish this investment, rather than requiring new skills/knowledge?		25
	Degree to which this investment produces positive side effects (e.g., enhancing brand/reputation, building customer trust, benefiting supply chain partners)?		27

	Category / Indicator	Cat Rank (1-7)	Ind Rank (1-33)
Cat	**Involvement**	5	
Consider	What level of involvement and buy-in are required from various parties for investment success -- both within and outside of the organization?		
Indicators	Level of buy-in required throughout the organization? (Must all employees be on board 100% for this to work? Or only a subset, such as management and certain key employees?)		12
	To what extent does this investment require the active involvement of many departments across the organization?		21
	Number of people who need to be actively involved?		24
	Level of involvement by third parties required (partners, consultants, vendors, etc.)?		13
	Degree of external, independent assessment/auditing (vs. in-house assessment/auditing) required?		30

	Category / Indicator	Cat Rank (1-7)	Ind Rank (1-33)
Cat	**Measurability**	7	
Consider	How measurable is the outcome of this investment?		
Indicators	Degree to which this investment can be evaluated using existing approaches and reporting mechanisms?		32
	What is the measurability of the outcome? Can it be quantified in tangible terms (revenue, market share, stock price, etc.)?		31
	If the outcome is intangible (e.g., goodwill, increased customer trust, enhanced brand), can the benefits be demonstrated against meaningful business success factors?		33

	Category / Indicator	Cat Rank (1-7)	Ind Rank (1-33)
Cat	**Time and effort required**	4	
Consider	(1) What level of staff-hours will be required to accomplish this investment?		
	(2) How long will it take to reach break-even cost for this investment?		
Indicators	Board of directors time required?		17
	Senior management time required?		18
	Cross-organizational team/steering committee time required?		19
	Middle and lower management time required?		23
	Other key staff time required?		22
	Time likely needed to achieve the required level of buy-in?		14
	Time required to achieve first demonstrated results of task?		26
	Time required to achieve full adoption and use of investment results across all affected business units?		15
	Time to achieve breakeven, if quantifiable?		8

A.2 Scores for One Investment in One Category

In this example and for the investment being considered, the answer to the Cost category question "What is the estimated total cost of accomplishing this investment . . ." is low. So the word "low" is replaced by the number "4" (indicated at the top of the column) to allow for a numeric calculation. Given the weighting factors that are applied based on the category rank, the score for the Cost category is calculated to be "4." This score is added to the other six category scores to arrive at the CAT TOTAL score that appears in Appendix A.3[35].

The indicators are assigned the following values and corresponding scores:

- Overt cost at outset is medium, so the word "med" is replaced by the number "3" and a resulting score of "3" is calculated based on the indicator rank.

35. #dsy985-BSI_a.3

- Estimated life cycle cost is very low, so the word “v low” is replaced by the number “5” and a resulting score of “3.75” is calculated.
- Cost of NOT doing this investment is high, so the word “high” is replaced by the number “4” and a resulting score of “4” is calculated.
- Potential cost savings is high, so the word “high” is replaced by the number “4” and resulting score of “3” is calculated.

These indicator scores are added to the other 29 indicator scores for this investment to produce the IND TOTAL score that appears in Appendix A.3[36].

The red, orange, yellow, light green, and green colors and text are intended to serve as visual cues. Questions that have category and indicator answers that tend to the red end of the spectrum will likely result in a “don’t do” this investment decision. Questions that have category and indicator answers that tend to the green end of the spectrum will likely result in a “do” this investment decision.

				1	2	3	4	5		
	Category / Indicator	Cat Rank (1-7)	Ind Rank (1-33)	don't do	unlikely	later?	soon	do	MULT	SCORE
Cat	Cost	2		v high	high	med	4	v low	4	4
Consider	What is the estimated total cost in dollars of accomplishing this investment, taking into account the potential cost savings and/or risk reduction to the organization?									
Indicators	Overt cost in dollars at outset to accomplish this investment?		6	v high	high	3	low	v low	3	3
	Estimated life cycle cost in dollars over time to sustain this investment?		7	v high	high	med	low	5	5	3.75
	Cost of NOT doing this investment, in terms of potential exposure and residual risk (high = investment is more necessary)?		1	v low	low	med	4	v high	4	4
	Potential cost savings to organization beyond breakeven point, if quantifiable (ROI), over time? (high = better)		9	v low	low	med	4	v high	4	3

A.3 Summary Results for Four Investments

Summary results are calculated as follows:

- CAT TOTAL: the numeric sum of the scores for all 7 categories
- IND TOTAL: the numeric sum of the scores for all 33 indicators
- TOP 6 TOTAL: the numeric sum of the scores for the 6 highest priority indicators. This provides an alternative view in the event that 6 specific indicators are of equal or greater relevance to the investment decision.

The “Overall Summary View” provides a bar chart comparison of CAT TOTAL, IND TOTAL, and TOP 6 TOTAL. The elements of the Summary View are then displayed individually in the following Summary displays.

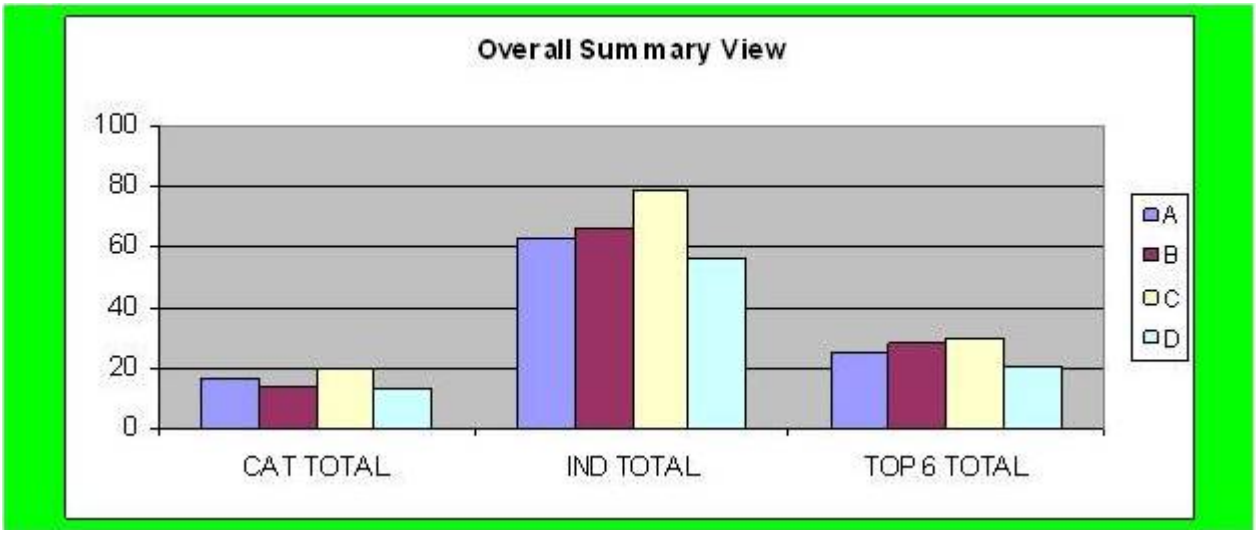
In this particular example, Investment C: *Integrate the use of static code analysis tools into the standard SDLC* has the highest score (sum of CAT TOTAL and IND TOTAL; confirmed by TOP 6 TOTAL) so should be considered as the first software assurance investment to fund. It is closely followed by Investment B: *Integrate secure coding practices for C and C++ into the standard SDLC*, which should be funded next assuming funds are available. Investment A: *Integrate architectural risk analysis into the standard SDLC* and Investment D: *Integrate security requirements engineering using SQUARE into the SDLC* are next in line respectively, subject to available resources.

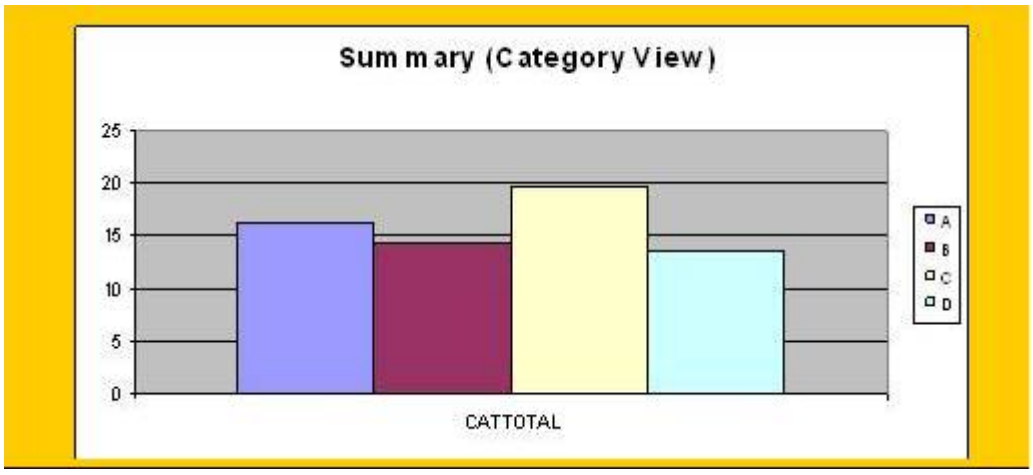
36. #dsy985-BSI_a.3

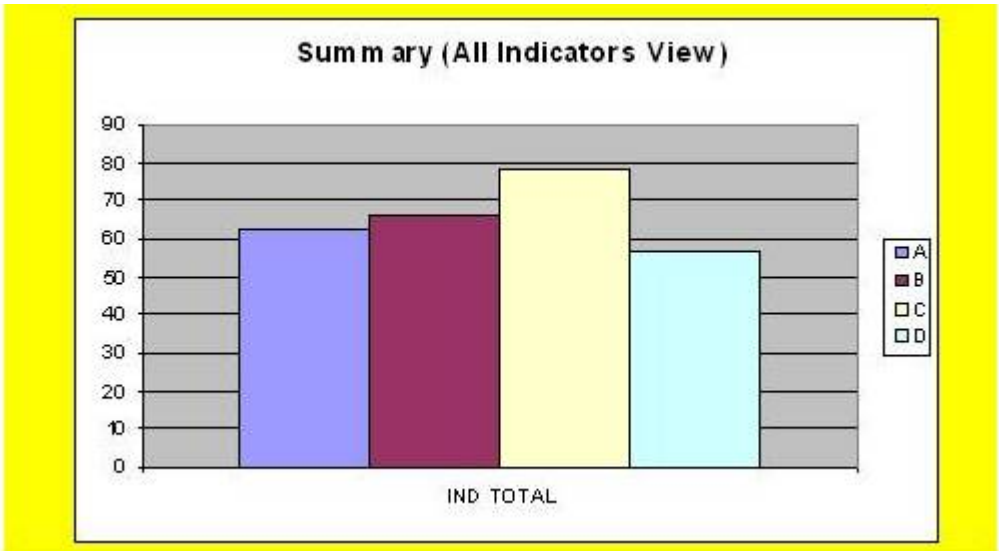
DASHBOARD SAMPLE

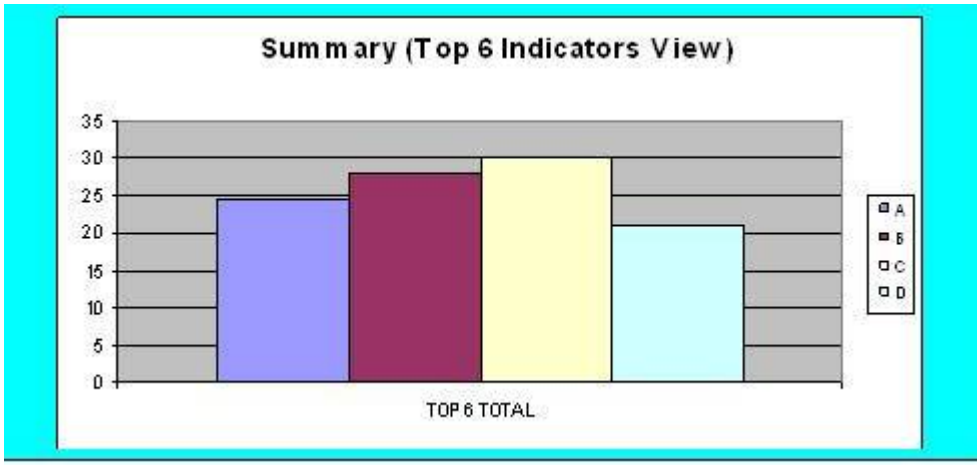
	Candidate Investments								
	A	B	C	D	etc.				
CAT TOTAL	16.25	14.25	19.75	13.5					
IND TOTAL	62.5	66.25	78.75	56.5					
TOP 6 TOTAL	24.75	28	30	21					

Project	Description
A	Integrate architectural risk analysis into the standard SDLC
B	Integrate secure coding practices into the standard SDLC
C	Integrate static code analysis into the standard SDLC
D	Integrate security requirements engineering using SQUARE into the SDLC









Carnegie Mellon Copyright

1. mailto:permission@sei.cmu.edu